



Maryland State Board of Elections Information System Security Plan (ISSP)

Maryland State Board of Elections

Pamela Woodside, CIO

September 30, 2004

Classification: Public

Agenda

- History
- HAVA 2002
- State Board of Elections Mission
- Risk Assessments
- Voter Confidence
- Security Objectives
- ISSP Objectives
- ISSP Plan Development
- Summary

Help America Vote Act 2002 (HAVA)

Implement Election Reform

- 1. Using a voting system that meets the minimum requirements of the Act;**
- 2. Mandating provisional voting;**
- 3. Creating a statewide, central voter registration system;**
- 4. Requiring certain voters to satisfy an identification requirement before voting;**
- 5. Requiring certain information be posted on Election Day; and**
- 6. Establishing an administrative complaint procedure for handling alleged violations of Title III of the Help America Vote Act.**

State Board of Elections Mission

The mission of the State Board is to provide all eligible citizens of the State convenient access to voter registration; to provide all registered voters accessible locations in which they may exercise their right to vote, to ensure uniformity of election practices; to promote fair and equitable elections; and to maintain registration records, campaign fund reports, and other election-related data accurately and in a form that is accessible to the public.

Maryland State Board of Elections

Mission

- Supervise the conduct of elections in the State;
- Direct, support, monitor, and evaluate the activities of each local board;
- Adopt regulations to implement its powers and duties;
- Receive, and in its discretion audit, the campaign finance reports and statements required under Title 13 of the Election Law Article;
- Maximize the use of technology in election administration, including the development of a plan for a comprehensive computerized elections management system;

Maryland State Board of Elections

Mission

- Canvass and certify the results of elections as prescribed by law;
- Make available to the general public, in a timely and efficient manner, information on the electoral process, including a publication that includes the text of the Election Law Article, relevant portions of the Maryland Constitution, and information gathered and maintained regarding elections;
- Receive, maintain, and serve as a depository for elections documents, materials, records, statistics, reports, certificates, proclamations, and other information prescribed by law or regulation; and
- Prescribe all forms required under the Election Law Article.

Hopkins Study

Dr. Avi Rubin,
Technical Director John's Hopkins Information Security Institute,
Hopkins Study, July 23, 2003

- * Reviewed Source Code
- * Focused on Smart cards, Cryptography, Configuration and Software Engineering
- * Revealed security flaws with AccuVote TS Systems

SAIC Report

- September 2, 2003
- NIST SP 800-30, *Risk Management Guide for IT Systems*
- Risk Assessment of AccuVote voting systems
- Evaluation of threats, vulnerabilities, security controls
- Measured the level of assurance of security controls
- “Dr. Rubin did not have a complete understanding of Maryland’s implementation, process controls and environment.”
- Contains sensitive security information and not for public disclosure

RABA Report Jan 20, 2004

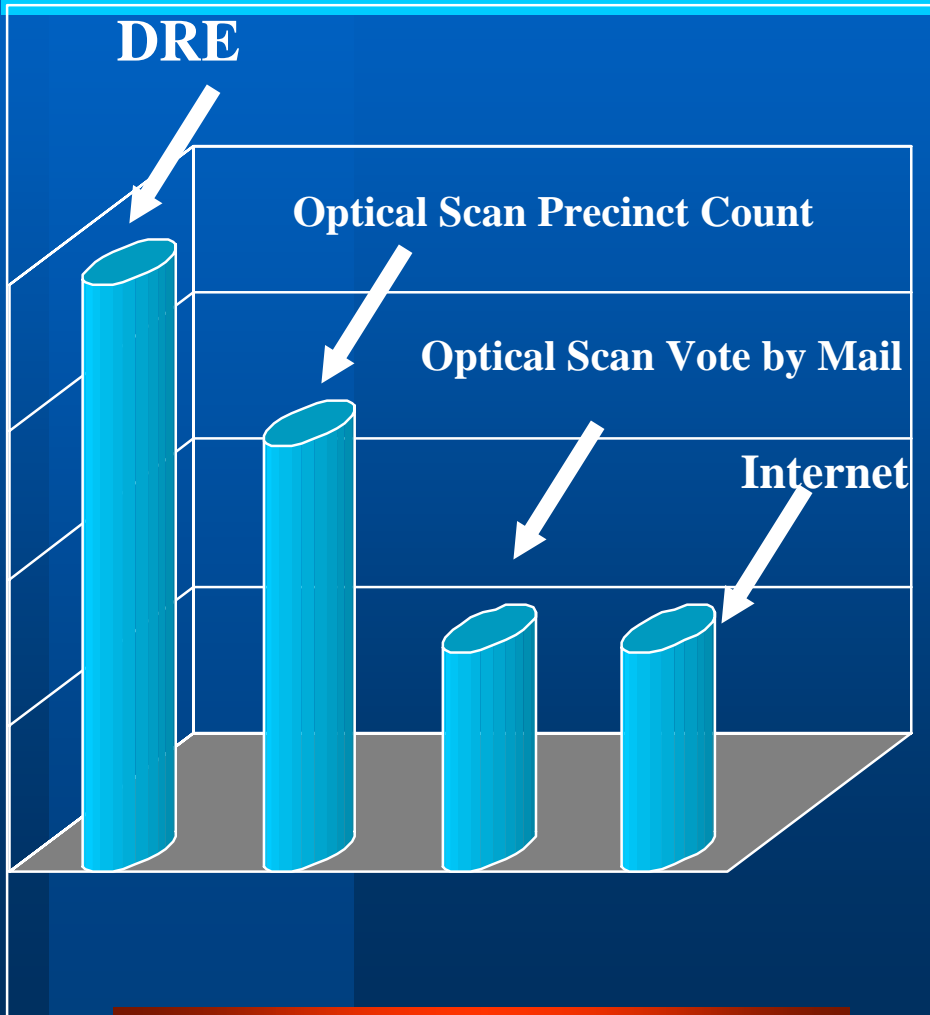
Examine and critique:

- The methodology and practices used by SAIC
- The conclusions reached by SAIC regarding integrity of the Diebold voting machines
- The Hopkins Study (Rubin Report)
- The IT Security Certification and Accreditation Guidelines as issued by DBM

Assist:

- DLS in comparing existing SBE practices and procedures to those counterparts in other states

Public Attitude Toward Voting Systems Confidentiality and Accuracy



- Very High Trust in DRE
- Followed by Optical Scan in Precinct and by Optical Scan by Mail
- Internet Voting Least Acceptable to Voters

Maintaining Public Confidence

- Create an Information Security Plan that proactively addresses and mitigates a series of voting system security issues
- Published a high level progress report on the SBE Website for public viewing
- Update DLS on our progress
- Address the Media

FEC Security Objectives

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized
- To protect the system from intentional manipulation and fraud, and from malicious mischief

State Board of Elections Security Objectives

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized
- To protect the system from intentional manipulation and fraud, and from malicious mischief

State Board of Elections Security Objectives

- To identify fraudulent or erroneous changes to the system
- To protect secrecy in the voting process

ISSP Creation

- Became apparent a formal plan was needed
- Attempt to move from reactive to proactive
- Based on SBE and other Risk Assessments
- Not only Voting Systems but supporting IT Infrastructure and Voter Registration
- Used In-house security expertise, CISSP and Security Consulting firm with CISSP credentials

ISSP Creation

- Needed to align plan with objectives
- Needed to identify mission critical systems and applications
- Needed to be realistic
 - Used Risk Assessments as a basis

NIST Guideline for ISSP

**Guide for Developing Security Plans for
Information Technology Systems,
800-18 states:**

The purpose of the security plan is to provide an overview
of the security requirements of the system and describe the
controls in place or planned for meeting those requirements;

and

Delineates responsibilities and expected behavior

<http://csrc.nist.gov/publications/nistpubs/>

Plan Development

- Plan can address both Major Application or General Support System (LAN)
- Includes Rules of Behavior
- System Analysis
- System Boundaries
- Identify System Owners
- Operational Status
- Interconnections
- Sensitivity of Information Handled
- Risk Assessment, Vulnerability Assessment
- Physical Security
- Contingency Planning

ISSP Components

ISSP

Managerial, Operational and Technical Controls

Voting Systems

AccuVote Touch Screen
GEMS Servers
Encoders
Smart Cards
Software
Firmware

Voter Registration

Servers
Applications

System Interfaces
With
Other Agencies

IT Infrastructure

Local Area Network
Work Stations
Servers, Firewall, Routers
Applications
Service Providers
E-mail, Web Services

ISSP Summary

- **Ensure Plan is consistent with your Agency's objectives**
- **Put your plan in place before others do it for you**
- **Utilize NIST Guidelines**
- **Follow-up with plan recommendations**
- **Remember that System Sensitive Information is classified non-public**

ISSP Summary

- Questions?